UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,029	11/04/2003	Brian Grove	G&C 30074.50-US-U1	6164

23973 7590 04/08/2009

DRINKER BIDDLE & REATH
ATTN: INTELLECTUAL PROPERTY GROUP
ONE LOGAN SQUARE
18TH AND CHERRY STREETS
PHILADELPHIA, PA 19103-6996

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
04/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Examiner-Initiated Interview Summary

Application No.	Applicant(s)	
10/701,029	GROVE ET AL.	
Examiner	**Art Unit**	
ELENI A. SHIFERAW	2436	

All Participants:

(1) *ELENI A. SHIFERAW*.

(2) *Gregory J. Lavorgna*.

Status of Application: _____

(3) _____.

(4) _____.

Date of Interview: *1 April 2009*

Time: _____

Type of Interview:
☒ Telephonic
☐ Video Conference
☐ Personal (Copy given to: ☐ Applicant ☐ Applicant's representative)

Exhibit Shown or Demonstrated: ☐ Yes ☐ No
If Yes, provide a brief description: .

Part I.

Rejection(s) discussed:

Claims discussed:

Prior art documents discussed:

Part II.

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:
See Continuation Sheet

Part III.

☐ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.
☒ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

/Eleni A Shiferaw/
Examiner, Art Unit 2436

(Applicant/Applicant's Representative Signature – if appropriate)

Continuation of Substance of Interview including description of the general nature of what was discussed:
The examiner contacted the applicant's undersigned attorney Gregory J. Lavorgna to move the case forward by providing proposed amendment as follows below, Mr. Lavorgna called back on 4/2/09 and said the inventor thinks it will narrow the invention since there might be some more unique characteristics in the feature and it will limit the inventor from those feature unique characteristics. The examiner's intention was to expedite the prosecution and move the case forward.

34. (Currently Amended) A method of authenticating a hardware token for operation with a host, comprising:
retrieving a value X from a memory separate from the hardware token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a hash of concatenated computed at least in part from non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server, to authenticate the hardware token;
wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;
wherein the value X is computed in the hardware token, according to X = f(P, F), wherein f(P, F) is a reversible function such that f(f(P, F), F) = P, wherein f(P, F) further comprises P XOR F, and stored in the host;
re-computing the fingerprint F;
regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and
transmitting the regenerated identifier P to the hardware token to unlock authenticate the hardware token for operation with the host.

36. (Canceled)

38. (Canceled)

39. (Canceled)

40. (Canceled)

44. (Currently amended) The method of claim 34, wherein:
the authorizing entity is a host computer communicatively coupleable to the hardware token; and
the value X is stored in the host computer.

45. (Currently amended) The method of claim 34, wherein the value X is stored in a memory accessible to the authentication entity by performing steps comprising the steps of:
computing a reference value H associated with the value X; and
associably storing the value X and the reference value H in a memory of the hardware token.

48. (Currently Amended) The method of claim 45, wherein the reference value H is computed at least in part from [[a]] the hash of the fingerprint F.

49. (Currently Amended) An apparatus for authenticating a hardware token for operation with a host, comprising:
a memory;
means for retrieving a value X from [[a]] the memory separate from the hardware token accessible to an authenticating entity, the value X generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a hash of concatenated computed at least in part from non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server, to authenticate the hardware token;
wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;
wherein the value X is computed in the hardware token, according to X = f(P, F), wherein f(P, F) is a reversible function such that f(f(P, F), F) = P, wherein f(P, F) further comprises P XOR F, and stored in the host;
re-computing the fingerprint F;
means for regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and
means for transmitting the regenerated identifier P to the hardware token to unlock authenticate the hardware token for operation with the host.

51. (Canceled)
53. (Canceled)
54. (Canceled)
55. (Canceled)
59. (Currently amended) The apparatus of claim 49, wherein:
the authorizing entity is a host computer communicatively coupleable to the hardware token; and
the value X is stored in the host computer.
60. (Currently amended) The apparatus of claim 49, wherein the value X is stored in a memory
of the hardware token, and wherein the hardware token further comprises:
means for computing a reference value H associated with the value X; and
means for associably storing the value X and the reference value H in a memory of the hardware token.
63. (Currently Amended) The apparatus of claim 60, wherein the reference value H is computed at least in part from [[a]] the hash of the fingerprint F.
64. (Currently Amended) An apparatus for authenticating a hardware token for operation with a host, the apparatus comprising a processor and a memory storing instructions for performing steps comprising the steps of:
retrieving a value X from a memory separate from the hardware token accessible to an
authenticating entity, the value X generated from a non-yawing computer fingerprint F of the host and an identifier P securing access to the hardware token, wherein the host fingerprint F is a hash of concatenated computed at least in part from non-varying host information C based on a unique characteristic of the host and a server specific value V transmitted from the server, to authenticate the hardware token;
wherein the concatenated non-varying host information C includes a host processor serial or model number, hard disk serial or model number, a network interface MAC address or unique serial number burned into Ethernet and token ring adaptor, basic input output system code area checksum and operating system type or version;
wherein the value X is computed in the hardware token, according to X = f(P, F), wherein f(P, F) is a reversible function such that f(f(P, F), F) = P, wherein f(P, F) further comprises P XOR F, and stored in the host;
re-computing the fingerprint F;
regenerating the same identifier value P for the hardware token at least in part from the retrieved value X and the re-computed fingerprint F; and
transmitting the regenerated identifier P to the hardware token to unlock authenticate the hardware token for operation with the host.

66. (Canceled)
68. (Canceled)
69. (Canceled)
70. (Canceled)
74. (Currently amended) The apparatus of claim 64, wherein:
the authorizing entity is a host computer communicatively coupleable to the hardware token; and
the value X is stored in the host computer.
75. (Currently amended) The apparatus of claim 64, wherein the value X is stored in a memory
of the hardware token, and the processing steps further comprise the steps of:
computing a reference value H associated with the value X; and
associably storing the value X and the reference value H in a memory of the hardware token.
78. (Currently amended) The apparatus of claim 75, wherein the reference value H is computed at least in part from [[a]] the hash of the fingerprint F.
.